

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ D'COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
4 septembre 2003 (04.09.2003)

PCT

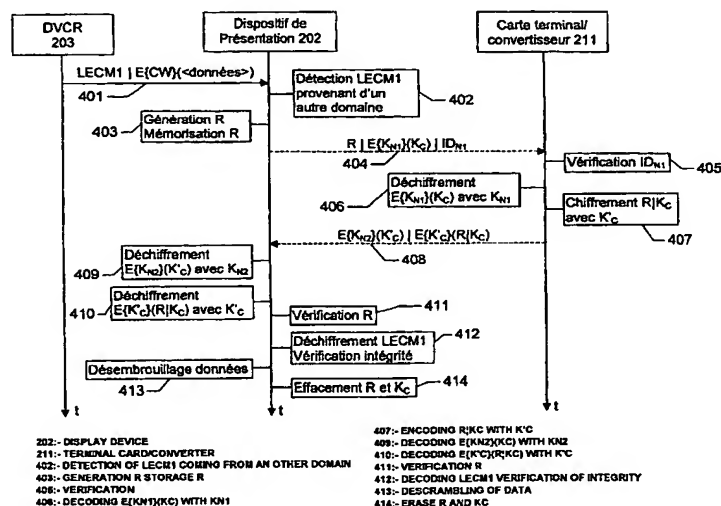
(10) Numéro de publication internationale  
WO 03/073761 A1

- (51) Classification internationale des brevets<sup>7</sup> : H04N 7/16, 7/167
- (72) Inventeur; et  
(75) Inventeur/Déposant (pour US seulement) : DURAND, Alain [FR/FR]; 79, rue de Dinan, F-35000 Rennes (FR).
- (21) Numéro de la demande internationale : PCT/FR03/00583
- (74) Mandataire : BERTHIER, Karine; THOMSON, 46 Quai Alphonse Le Gallo, F-92648 Boulogne cedex (FR).
- (22) Date de dépôt international : 21 février 2003 (21.02.2003)
- (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité : 02/02330 25 février 2002 (25.02.2002) FR
- (71) Déposant (pour tous les États désignés sauf US) : THOMSON LICENSING S.A. [FR/FR]; 46 Quai Alphonse Le Gallo, F-92100 Boulogne Billancourt (FR).
- (84) États désignés (régional) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: METHOD FOR PROCESSING ENCODED DATA FOR A FIRST DOMAIN RECEIVED IN A NETWORK PERTAINING TO A SECOND DOMAIN

(54) Titre : PROCÉDE DE TRAITEMENT DE DONNÉES CHIFFRÉES POUR UN PREMIER DOMAINE ET REÇUES DANS UN RESEAU APPARTENANT A UN SECOND DOMAINE



(57) Abstract: The invention relates to a method for processing data (LECM1), encoded by means of an encoding process unique to a first domain such that said data may not be decoded other than by means of a first secret (KN1) unique to the first domain. Said data are received in a display device (202) connected to a network pertaining to a second domain. The method comprises the following steps for the display device of: (a) transmitting (404) at least one part (E{KN1}(KC)) of said encoded data to a processing device (211) connected to the network; (b) receipt (408) from said processing device (211) of at least one element (E{KN2}(K'C)E{K'C}(KC)) for decoding said received data by means of a second secret (KN2) unique to the second domain, said second secret begin held in the display device.

[Suite sur la page suivante]



européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

**Déclarations en vertu de la règle 4.17 :**

- relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US
- relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** L'invention concerne un procédé de traitement de données (LECM1), chiffrées selon un procédé de chiffrement propre à un premier domaine de sorte qu'elles ne puissent être déchiffrées qu'à l'aide d'un premier secret (KN1) propre au premier domaine, ces données étant reçues dans un dispositif de présentation (202) raccordé à un réseau appartenant à un second domaine. Le procédé comporte les étapes consistant pour le dispositif de présentation à : (a) transmettre (404) à un dispositif de traitement (211) raccordé au réseau une partie (E{KN1}(KC)) au moins desdites données chiffrées ; (b) recevoir (408) dudit dispositif de traitement (211) au moins un élément (E{KN2}(K'C)|E{K'C}(KC)) permettant de déchiffrer lesdites données reçues à l'aide d'un second secret (KN2) propre au second domaine, le second secret étant contenu dans le dispositif de présentation.

**Procédé de traitement de données chiffrées pour un premier domaine et  
reçues dans un réseau appartenant à un second domaine**

**Domaine de l'invention**

5           La présente invention concerne le domaine de la protection contre la copie de données numériques et contre l'accès illégal à de telles données, en particulier dans le cas de données circulant dans des réseaux numériques locaux tels des réseaux domestiques numériques.

10           **Etat de la technique**

          Il est connu dans le contexte de la protection contre la copie illicite de données numériques des systèmes dans lesquels un contenu numérique peut être copié pour être utilisé dans un domaine déterminé. On entend par domaine un ensemble d'appareils appartenant par exemple à un même réseau  
15 domestique, ces appareils partageant un secret propre au domaine, par exemple une clé de chiffrement cryptographique. Un appareil appartenant à un domaine peut être un appareil portable. Son appartenance à un domaine particulier sera déterminée par sa connaissance du secret propre à ce domaine particulier.

20           Les contenus numériques dans un tel domaine peuvent être de trois sortes :

          - « copie libre » : ce type de contenu peut être enregistré et relu dans n'importe quel domaine, il n'est donc pas nécessaire de connaître un secret propre à un domaine pour lire ce type de contenu ;

25           - « copie privée » : ce type de contenu ne peut être copié que pour un domaine particulier dans lequel il pourra être relu ; le contenu est enregistré sous une forme qui nécessite la connaissance du secret du domaine particulier pour pouvoir être relu. Ce type de contenu ne peut pas être lu sur un appareil qui n'appartient pas au domaine particulier.

30           - « lecture seule » : ce type de contenu peut seulement être lu dans un domaine particulier mais il ne peut pas être copié ; ou si des copies du contenu sont effectuées, celles-ci ne pourront pas être relues ensuite.

          Un contenu numérique entre généralement dans un domaine à travers un dispositif d'accès ou dispositif source. Ce type de dispositif récupère  
35 des données numériques à travers un canal externe au domaine et les diffuse aux autres dispositifs du domaine, par exemple grâce à un bus numérique reliant les différents appareils du domaine. Un dispositif source peut notamment être un décodeur numérique destiné à recevoir des programmes vidéo de

l'extérieur d'un réseau domestique numérique, via une antenne satellite ou une connexion au câble, pour les diffuser dans le réseau. Il peut également s'agir d'un lecteur de disque optique diffusant dans un réseau domestique des données (audio et/ou vidéo) lues sur un disque optique (le disque contient dans ce cas des données provenant de l'extérieur du réseau).

A l'intérieur du domaine, les contenus numériques peuvent être enregistrés par des dispositifs d'enregistrement numériques, tels un enregistreur DVD (de l'anglais « Digital Versatile Disc » signifiant littéralement « Disque Polyvalent Numérique ») ou un disque dur.

10 Finalement, le contenu est présenté aux utilisateurs du domaine par des dispositifs de présentation. Ces dispositifs sont adaptés à recevoir les contenus du domaine (notamment les données numériques circulant dans un réseau domestique numérique) pour les traiter (notamment pour les décrypter si nécessaire) et les présenter à l'utilisateur final. Il s'agit notamment de  
15 récepteurs de télévision permettant de visualiser des données vidéo ou d'appareils Hi-Fi pour écouter des données audio.

Un dispositif source contient généralement un module dit « d'accès conditionnel » ou un module de gestion des droits numériques (dit « module DRM » pour « Digital Rights Management ») selon que le contenu est  
20 respectivement un contenu « diffusé » (« broadcast content » en anglais) ou un contenu « large bande » (« broadband content » en anglais). Ces modules gèrent la protection du contenu mise en place par le fournisseur de contenu.

Par exemple, si l'on considère des programmes télévisés payants, le fournisseur de contenu, c'est à dire le diffuseur de programmes, fournit  
25 habituellement les programmes numériques sous une forme embrouillée (c'est à dire cryptée) à l'aide de clés appelées mots de contrôle, les mots de contrôle étant eux-mêmes transmis avec les données sous forme chiffrée dans des messages appelés « ECM » (de l'anglais « Entitlement Control Message » signifiant littéralement « Message de Contrôle des Droits »). Le fournisseur de  
30 contenu fournit également aux abonnés ayant payé pour recevoir les programmes la clé permettant de déchiffrer les mots de contrôle et un module d'accès conditionnel contenant, entre autre, l'algorithme de déchiffrement des mots de contrôle (la clé et le module d'accès conditionnel sont préférentiellement inclus dans une carte à puce). C'est aussi le fournisseur de  
35 contenu qui définit les règles d'utilisation du contenu fourni, c'est à dire qui définit si le contenu est du type « copie libre », « copie privée » ou « lecture seule ».

Dans le système de protection contre la copie connu sous le nom de *SmartRight™* (*SmartRight* est une marque déposée de la société THOMSON multimedia), les dispositifs sources transforment les contenus reçus en fonction des règles d'utilisation de ces contenus.

5           Lorsqu'un contenu reçu par un dispositif source d'un domaine donné est de type « copie privée », le contenu est transformé de manière à ce qu'il ne puisse être décrypté que par des dispositifs de présentation appartenant à ce domaine particulier (et donc partageant tous un même secret). La demande de brevet français No. 01 05568, déposée le 25 avril 2001 au nom du demandeur  
10 THOMSON Licensing S.A., concernant un procédé de gestion de clé symétrique dans un réseau de communication, décrit notamment comment cette transformation est effectuée de sorte que seuls les dispositifs de présentation connaissant une clé secrète du réseau de communication sont capables de décrypter le contenu pour le lire.

15           On notera que, dans la suite de la description, les termes « clé secrète » ou « clé symétrique » seront utilisés pour désigner une clé cryptographique utilisée dans un algorithme de chiffrement ou de déchiffrement symétrique, tel que l'algorithme connu sous le nom de AES (acronyme de « Advanced Encryption Standard ») ou encore sous le nom de « Rijndael » et  
20 décrit notamment dans le document « *Proceedings from the first Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST), août 1998, J. Daemen et V. Rijmen* ».

Lorsqu'un contenu reçu par un dispositif source est de type « lecture seule », le contenu est également transformé par ce dispositif source en  
25 utilisant le procédé décrit dans la demande de brevet précitée de sorte qu'il ne puisse être lu que par les dispositifs de présentation du réseau qui connaissent la clé secrète du réseau. De plus, un procédé décrit dans la demande de brevet français No. 00 15894, déposée le 7 décembre 2000 au nom de THOMSON multimedia, est mis en œuvre pour que le contenu ne puisse pas être copié  
30 dans le domaine ou qu'en cas de copie, celle-ci ne puisse pas être relue par les dispositifs de présentation du domaine.

Lorsqu'un contenu reçu dans un domaine est de type « copie libre », il est généralement en clair et est laissé sous cette forme par le dispositif source qui a reçu le contenu pour le diffuser dans le domaine.

35           Grâce à ce système, il est possible à un utilisateur qui reçoit un contenu après avoir payé au fournisseur de ce contenu les droits associés, de garder une copie privée de ce contenu pour son usage personnel ultérieur.

Cette copie ne pourra être lue que par des dispositifs de présentation de son domaine, c'est à dire du domaine dans lequel le contenu a été reçu initialement.

Néanmoins, il existe des cas dans lesquels il est souhaitable de pouvoir relire une copie privée effectuée dans un premier domaine sur un  
5 dispositif de présentation d'un second domaine. Notamment, si un utilisateur souhaite visualiser sur le domaine d'un ami la copie d'un film effectuée sur son propre domaine, naturellement sans qu'une copie puisse être réalisée pour le domaine de l'ami.

Ceci peut également être nécessaire en cas d'union ou de  
10 séparation d'utilisateurs. En cas d'union, si chaque utilisateur avait auparavant son propre domaine, les deux domaines ne pourront être reliés ensemble car les appareils des deux domaines ne partagent pas le même secret. Dans ce cas, si les deux utilisateurs ne veulent pas gérer deux domaines différents, il  
15 faudra que les contenus enregistrés au préalable sur un premier domaine puissent être relus sur le deuxième domaine. De même, lorsque l'on souhaite séparer un domaine en deux domaines différents (parce que des époux se séparent ou qu'un enfant quitte le domicile de ses parents), il est nécessaire de pouvoir relire les contenus enregistrés au préalable sur le domaine commun sur  
les deux nouveaux domaines.

20 La présente invention vise à résoudre les problèmes précités.

#### Exposé de l'invention

L'invention concerne à cet effet, un procédé de traitement de données, chiffrées selon un procédé de chiffrement propre à un premier  
25 domaine de sorte qu'elles ne puissent être déchiffrées qu'à l'aide d'un premier secret propre audit premier domaine, lesdites données étant reçues dans un dispositif de présentation raccordé à un réseau appartenant à un second domaine. Selon l'invention, le procédé comporte les étapes consistant pour le dispositif de présentation à :

30 (a) transmettre à un dispositif de traitement raccordé au réseau une partie au moins desdites données chiffrées ;

(b) recevoir dudit dispositif de traitement au moins un élément permettant de déchiffrer lesdites données reçues à l'aide d'un second secret propre audit second domaine, ledit second secret étant contenu dans le  
35 dispositif de présentation.

Ainsi le déchiffrement des données est délégué à un dispositif de traitement qui connaît le premier secret propre au premier domaine et qui

effectue un traitement sur la partie des données qu'il reçoit de sorte que le dispositif de présentation du second domaine puisse déchiffrer les données reçues simplement en connaissant le second secret propre au second domaine.

De plus, comme le secret du premier domaine n'est pas transmis au  
5 dispositif de présentation du second domaine, il ne peut déchiffrer les données reçues que lorsque le dispositif de traitement est raccordé au réseau du second domaine.

Selon un mode de réalisation particulier de l'invention, les données  
reçues dans le dispositif de présentation sont chiffrées à l'aide d'une première  
10 clé symétrique, ladite première clé symétrique étant reçue avec les données sous forme chiffrée à l'aide du premier secret. Dans ce mode de réalisation, l'étape (a) consiste à transmettre au dispositif de traitement la première clé symétrique chiffrée à l'aide du premier secret ; et l'étape (b) consiste à recevoir  
du dispositif de traitement : la première clé symétrique chiffrée à l'aide d'une  
15 seconde clé symétrique ; et la seconde clé symétrique chiffrée à l'aide du second secret propre au second domaine.

Selon une caractéristique particulière de l'invention, le procédé comporte en outre les étapes consistant pour le dispositif de présentation à :

(c) déchiffrer, à l'aide du second secret, la seconde clé symétrique  
20 chiffrée ;

(d) déchiffrer, à l'aide de la seconde clé symétrique, la première clé symétrique chiffrée ; et

(e) déchiffrer les données reçues par ledit dispositif de présentation à l'aide de la première clé symétrique.

25 Selon un mode de réalisation particulier de l'invention, le procédé comporte en outre, avant l'étape (a), une étape consistant pour le dispositif de présentation à générer un nombre aléatoire, le nombre aléatoire étant transmis au dispositif de traitement, à l'étape (a), avec le chiffrement de la première clé symétrique. Dans ce mode de réalisation les données reçues à l'étape (b)  
30 contiennent un nombre aléatoire et la première clé symétrique chiffrés à l'aide de la seconde clé symétrique ; l'étape (d) comprend également le déchiffrement, à l'aide de la seconde symétrique, du nombre aléatoire chiffré reçus à l'étape (b) ; et le procédé comporte en outre, avant l'étape (e), une étape de vérification que le nombre aléatoire déchiffré à l'étape (d) est identique  
35 au nombre aléatoire généré avant l'étape (a) ; l'étape (e) n'étant effectuée qu'en cas de vérification positive.

Selon une autre caractéristique de l'invention, un identifiant de domaine est contenu dans les données reçues par le dispositif de présentation ;

l'identifiant de domaine est transmis au dispositif de traitement lors de l'étape (a) ; et l'étape (b) n'est effectuée que si le dispositif de traitement contient le même identifiant de domaine.

5                    Brève description des dessins

D'autres caractéristiques et avantages de l'invention apparaîtront à travers la description de modes de réalisation particuliers non limitatifs, explicités à l'aide des figures jointes, parmi lesquelles :

- la figure 1 est un schéma bloc d'un réseau domestique numérique  
10    raccordant entre eux des dispositifs appartenant à un premier domaine ;
- la figure 2 est un schéma bloc d'un réseau domestique comportant des dispositifs appartenant à un second domaine illustrant un mode de réalisation de l'invention ;
- la figure 3 est un diagramme temporel illustrant des échanges de  
15    clés entre deux dispositifs du réseau domestique de la figure 2 ;
- la figure 4 est un diagramme temporel illustrant les échanges de données entre des dispositifs du réseau domestique de la figure 2 permettant de lire (sans le copier) dans le second domaine, un contenu enregistré dans le  
20    premier domaine.

20                    Description détaillée de modes de réalisation de l'invention

Nous décrirons dans un premier temps, en liaison avec la figure 1, un exemple de réseau domestique dans lequel est mis en œuvre un système de protection contre la copie permettant d'effectuer des copies privées des  
25    contenus numériques, pour un usage futur uniquement dans le réseau domestique dans lequel ils ont été copiés.

Le réseau comprend un dispositif source 1, un dispositif de présentation 2 et un dispositif d'enregistrement 3 reliés ensemble par un bus numérique 4, qui est par exemple un bus selon la norme IEEE 1394.

30                    Le dispositif source 1 comprend un décodeur numérique 10 doté d'un lecteur de carte à puce muni d'une carte à puce 11. Ce décodeur reçoit des données numériques, notamment des programmes audio/vidéo distribués par un prestataire de service.

Le dispositif de présentation 2 comprend un récepteur de télévision  
35    numérique (DTV) 20 doté d'un lecteur de carte à puce muni d'une carte à puce 21 et le dispositif d'enregistrement 3 est notamment un magnétoscope numérique (DVCR).



Les données numériques qui entrent sur le réseau via le dispositif source 1 sont en général des données embrouillées par un fournisseur de contenu, par exemple selon le principe de la télévision payante. Dans ce cas, les données sont embrouillées à l'aide de mots de contrôle CW (de l'anglais « Control Word ») qui sont eux-même transmis dans le flux de données sous forme chiffrée à l'aide d'une clé de chiffrement  $K_F$  en étant contenus dans des messages de contrôle ECM (de l'anglais « Entitlement Control Message »). La clé de chiffrement  $K_F$  est mise à la disposition des utilisateurs qui ont payé pour recevoir les données, notamment en étant stockée dans une carte à puce.

5 Dans l'exemple de la figure 1, la carte à puce 11 contient une telle clé  $K_F$  ainsi qu'un module d'accès conditionnel CA 14 capable de déchiffrer les mots de contrôle CW.

Le dispositif source 1 qui reçoit ces données numériques embrouillées les met ensuite en forme pour qu'elles soient diffusées sur le réseau numérique selon un format de protection spécifique au réseau domestique. Le décodeur 10 comporte un module « unité ECM » 13 qui extrait du flux de données reçu les messages ECM contenant les mots de contrôle chiffrés à l'aide de la clé  $K_F$  pour les transmettre au module CA 14. Celui-ci déchiffre les mots de contrôle CW et les transmet à un module convertisseur 12 également contenu dans la carte à puce 11.

15 20

Le rôle du module convertisseur 12 est de transformer les informations contenues dans les messages ECM en messages LECM (de l'anglais « Local Entitlement Control Message ») protégés à l'aide d'une clé secrète spécifique au réseau domestique local, que l'on appellera la clé  $K_{N1}$ .

25 On suppose qu'auparavant le module convertisseur a généré aléatoirement une clé symétrique  $K_C$  et a requis le chiffrement de cette clé  $K_C$  à l'aide de la clé secrète du réseau  $K_{N1}$ . Le module convertisseur possède donc en mémoire la clé  $K_C$  et la clé  $K_C$  chiffrée par la clé secrète du réseau  $K_{N1}$  :  $E\{K_{N1}\}(K_C)$ .

30 Dans le reste de la description, on utilisera toujours la notation  $E\{K\}(M)$  pour signifier chiffrement avec une clé  $K$  des données  $M$ .

La demande de brevet français No. 01 05568 précitée décrit en détail le procédé qui permet au module convertisseur d'obtenir le chiffrement de la clé  $K_C$  à l'aide de la clé secrète du réseau  $K_{N1}$ , ce chiffrement étant effectué dans un dispositif de présentation. En effet, les dispositifs de présentation du réseau, tels que le dispositif 2 de la figure 1, sont les seuls à posséder la clé secrète du réseau  $K_{N1}$ . Celle-ci est contenue dans la carte à puce 21 avec un module

35

terminal 22 chargé, entre autre, des opérations de chiffrement et déchiffrement avec la clé du réseau  $K_{N1}$ .

Le fonctionnement du système est le suivant. Lorsque des données numériques sont reçues dans le décodeur 10, le module « unité ECM » 13 extrait les messages ECM contenant les mots de contrôle CW chiffrés à l'aide de la clé  $K_F$  spécifique au fournisseur de contenu et les fournit au module CA 14. Ce dernier déchiffre les mots de contrôle CW et les transmet au module convertisseur 12. De plus, le message ECM peut également contenir des informations de contrôle de la copie du contenu transmis indiquant si le contenu peut être copié librement ou non dans le réseau ou bien si le contenu peut seulement être visualisé (ou écouté...) dans le réseau. Ces informations sont également transmises au module convertisseur.

Le module convertisseur construit ensuite un message LECM à partir de ces données. Ce message comprend préférentiellement :

- une partie A en clair contenant notamment les informations de contrôle de la copie du contenu, c'est à dire indiquant si le contenu est de type « copie libre », « copie privée » ou bien « lecture seule » ; ces informations sont souvent notées VCI (acronyme de l'anglais « Viewing Control Information »). La partie en clair contient également la clé  $K_C$  chiffrée avec la clé du réseau :  $E\{K_{N1}\}(K_C)$ .

- une partie B, chiffrée avec la clé  $K_C$ , et contenant essentiellement le mot de contrôle déchiffré CW ; on peut résumer cette partie à :  $E\{K_C\}(CW)$ .

- un champ d'intégrité formé par le résultat d'une fonction de hachage appliquée à l'ensemble des parties A et B avant chiffrement de la partie B. Ce champ d'intégrité permet avantageusement de vérifier la validité des messages LECM et permet de s'assurer qu'ils ne sont pas modifiés illicitement.

Le message LECM est ensuite transmis à l'unité ECM qui l'insère dans le flux de données à la place des messages ECM. Il est à noter que lorsque le contenu reçu n'est pas déjà sous forme embrouillée comme décrit ci-dessus et ne contient pas de message ECM, le module convertisseur 12 est chargé dans ce cas de mettre les données sous cette forme pour que le flux de données diffusé sur le réseau 4 soit toujours sous la forme de paquets de données tels le paquet 40 représenté à la figure 1 contenant un message LECM et des données embrouillées.

On peut résumer le contenu de ce paquet comme suit :

LECM |  $E\{CW\}(<\text{données}>)$  ; soit :

$E\{K_{N1}\}(K_C)|VCI|E\{K_C\}(CW)|\text{Champ d'intégrité} | E\{CW\}(<\text{données}>)$  ;

où « | » représente l'opérateur de concaténation.

Lorsque ces paquets de données sont reçus par le récepteur de télévision numérique 20, ils sont transmis au module « Unité LECM » 23 qui en extrait les messages LECM pour les transmettre au module terminal 22. Ce dernier déchiffre tout d'abord  $E\{K_{N1}\}(K_C)$  à l'aide de la clé  $K_{N1}$  pour obtenir la clé  $K_C$ . Ensuite, à l'aide de la clé  $K_C$ , il déchiffre  $E\{K_C\}(CW)$  pour obtenir le mot de contrôle  $CW$  qu'il transmet au module « Unité LECM » 23. Celui-ci est alors en mesure de désembrouiller les données  $E\{CW\}(<\text{données}>)$  à l'aide du mot de contrôle. Les données désembrouillées sont ensuite présentées à l'utilisateur.

10 Dans le cas de données vidéo, celles-ci peuvent être visualisées sur le récepteur de télévision 20.

Si le flux de données contenant les paquets 40 est enregistré par le magnétoscope numérique 3 pour être relu plus tard, nous constatons que ceci n'est possible que si le dispositif de présentation sur lequel les données doivent

15 être présentées contient la clé secrète  $K_{N1}$  du domaine dans lequel les données ont été enregistrées. Nous appellerons dans la suite ce domaine  $N1$ .

Rappelons que nous entendons par domaine, dans l'exemple de la figure 1, le réseau domestique numérique ainsi que l'ensemble des appareils qui y sont connectés ainsi également que des appareils de présentation portables (non représentés) qui sont susceptibles d'être raccordés au réseau domestique et qui appartiennent aux membres de la famille possédant le

20 réseau domestique. Les appareils de présentation portables (par exemple des lecteurs de fichiers musicaux compressés) sont considérés comme faisant partie du domaine  $N1$  lorsqu'ils contiennent la clé secrète  $K_{N1}$ . On pourra se reporter à la demande de brevet français No. 01 05568 précitée pour y trouver une description de la manière dont la clé secrète du domaine  $N1$  est transmise aux nouveaux dispositifs de présentation qui « entrent » dans le domaine (par exemple lorsqu'un membre de la famille achète un nouvel appareil).

Supposons maintenant qu'un utilisateur ayant enregistré un contenu

30 (par exemple un film) de type « copie privée » sur son domaine  $N1$  souhaite pouvoir le visualiser sur un récepteur de télévision appartenant à un autre domaine que nous noterons  $N2$ .

Dans ce cas, l'utilisateur insérera par exemple une cassette contenant le film dans un magnétoscope numérique du domaine  $N2$ . Ce

35 magnétoscope diffusera le film sur le réseau domestique du domaine  $N2$  pour qu'il soit visualisé sur un récepteur de télévision du domaine  $N2$ . Mais comme ce dernier ne connaît pas la clé secrète du domaine  $N1$ ,  $K_{N1}$ , il ne pourra

déchiffrer le contenu des messages LECM et donc ne pourra pas désembrouiller les données pour présenter le film à l'utilisateur.

5 Nous allons maintenant décrire comment, grâce à l'invention, il sera possible de visualiser dans le domaine N2 le contenu enregistré comme « copie privée » dans le domaine N1 sans pour autant qu'il soit possible de réaliser une copie de ce contenu pour le domaine N2, ou du moins de manière à ce qu'en cas de copie dans le domaine N2, cette copie ne puisse pas être relue dans le domaine N2.

10 Pour cela, il est prévu un module spécial réunissant les fonctionnalités d'un module convertisseur et d'un module terminal et inclus préférentiellement dans une carte à puce. Nous parlerons dans la suite soit du module terminal/convertisseur, soit de la carte terminal/convertisseur.

15 Ce module devra d'abord être initialisé dans le domaine N1 pour recevoir le secret du domaine N1, à savoir la clé  $K_{N1}$ , puis il sera raccordé au domaine N2 pour réaliser le déchiffrement des parties chiffrées avec la clé  $K_{N1}$  des paquets de données formant le contenu.

Nous décrirons ci-dessous plus en détails comment ces étapes sont réalisées.

20 Sur la figure 2, nous avons représenté schématiquement le réseau domestique numérique d'un domaine N2 dans lequel est mis en œuvre le mode de réalisation préféré de l'invention. Nous n'avons représenté que les éléments nécessaires à la compréhension de l'invention.

25 Dans ce réseau, un bus numérique 204 relie entre eux un magnétoscope numérique 203, un dispositif de présentation 202 et un dispositif source 201. Le bus numérique 204 est préférentiellement un bus selon la norme IEEE 1394. Le dispositif de présentation 202 comprend un récepteur de télévision numérique DTV 220 qui comporte un module « Unité LECM » 223 et une carte à puce 221 comprenant un module terminal 222. Dans la carte à puce  
30 221 est mémorisée la clé secrète du domaine N2 :  $K_{N2}$ .

Le dispositif source 201 comprend un décodeur numérique 210 qui comporte un module « Unité ECM » 213. Dans le décodeur 210 se trouve insérée une carte terminal/convertisseur 211 qui comprend un module terminal 214 et un module convertisseur 212. Cette carte 211 est insérée à la place  
35 d'une carte « convertisseur », c'est à dire d'une carte à puce contenant un module convertisseur telle la carte 11 de la figure 1, dans le dispositif source 201.

En pratique, la carte terminal/convertisseur 211 appartient à l'utilisateur du domaine N1 et celui-ci l'insère dans un dispositif source (ou bien dans un dispositif de présentation comme on le verra dans un second mode de réalisation) du domaine N2 lorsqu'il souhaite visualiser dans le domaine N2 un contenu enregistré comme « copie privée » dans le domaine N1.

Le module terminal 214 contient la clé secrète du domaine N1 qu'il a reçu lors d'une phase d'initialisation de la carte terminal/convertisseur 211 dans le domaine N1.

En effet, avant d'être raccordée au réseau du domaine N2, la carte terminal/convertisseur 211 a été au préalable raccordée au réseau du domaine N1 en étant insérée dans un dispositif de présentation de N1 à la place de la carte « terminal » (une carte à puce contenant un module terminal telle la carte 21 de la figure 1) qui s'y trouve habituellement. Le module terminal 214 était alors considéré comme « vierge », c'est à dire n'appartenant à aucun domaine.

Le module terminal 214 a ensuite reçu du dispositif « géniteur » du domaine N1 la clé secrète  $K_{N1}$  avant de devenir « stérile ».

Les termes « vierge », « géniteur » et « stérile » sont définis dans la demande de brevet français No. 01 05568 précitée et désignent respectivement un dispositif de présentation (ou plus précisément son module terminal) :

- qui n'est raccordé à aucun domaine et ne contient aucune clé secrète de domaine (dispositif ou module terminal « vierge ») ;
- qui possède la clé secrète d'un domaine et peut la transmettre à un nouveau dispositif de présentation vierge susceptible d'être raccordé au domaine (dispositif ou module terminal « géniteur ») ; et
- qui possède la clé secrète d'un domaine mais ne peut pas la transmettre à un autre dispositif (dispositif ou module terminal « stérile »).

La demande de brevet précitée décrit également les mécanismes de transmission sécurisée de la clé secrète entre les différents dispositifs.

Après cette phase d'initialisation dans le domaine N1, la carte terminal/convertisseur 211 est donc raccordée à un domaine N2 dans lequel on souhaite visualiser un contenu enregistré comme « copie privée » dans le domaine N1. Sur la figure 2, elle est insérée dans le décodeur numérique 210 du dispositif source 201.

La figure 3 illustre les étapes qui sont mises en œuvre après que la carte terminal/convertisseur 211 a été raccordée au réseau du domaine N2.

Lors d'une première étape 100, une clé symétrique  $K'_C$  est générée aléatoirement par le module convertisseur 212 de la carte terminal/convertisseur 211 et est mémorisée dans la carte 211.

Lors de l'étape suivante 101, le dispositif source 201 diffuse sur le réseau du domaine N2 un message de requête pour recevoir une clé publique d'un dispositif de présentation du réseau. Chaque dispositif de présentation possède en effet une paire de clés asymétriques mémorisée dans la carte à puce qui contient le module terminal. Par exemple, le dispositif de présentation 202 de la figure 2 possède une clé publique  $K_{PUB\_T2}$  et une clé privée  $K_{PRI\_T2}$ . Ces clés sont utilisées de manière connue en soi pour réaliser des opérations de chiffrement ou de déchiffrement à l'aide d'algorithmes cryptographiques asymétriques (par exemple l'algorithme RSA, du nom de ses créateurs Rivest, Shamir et Adleman).

N'importe quel dispositif de présentation du domaine N2 peut répondre à cette requête 101. On suppose dans la suite que le dispositif de présentation 202 répond à la requête en envoyant sa clé publique  $K_{PUB\_T2}$  au dispositif source 201 lors de l'étape 102.

Le module convertisseur 212 réalise alors le chiffrement de la clé symétrique  $K'_C$  à l'aide de la clé publique  $K_{PUB\_T2}$  reçue (étape 103) puis il envoie le résultat de ce chiffrement  $E\{K_{PUB\_T2}\}(K'_C)$  au dispositif de présentation 202 (étape 104). Ce dernier déchiffre le résultat reçu à l'aide de sa clé privée  $K_{PRI\_T2}$  pour obtenir  $K'_C$  (étape 105). Il procède ensuite (étape 106) au chiffrement de  $K'_C$  avec la clé secrète du domaine N2,  $K_{N2}$ , pour obtenir  $E\{K_{N2}\}(K'_C)$ , résultat qu'il envoie au dispositif source 201 à l'étape 107. Ce résultat  $E\{K_{N2}\}(K'_C)$  est mémorisé dans la carte terminal/convertisseur 211 à l'étape suivante 108.

La carte terminal/convertisseur est maintenant prête à effectuer le déchiffrement du contenu de type « copie privée » du domaine N1 pour le domaine N2.

Nous allons maintenant décrire, en liaison avec la figure 4, le procédé mis en œuvre pour cela.

Sur la figure. 4, on a représenté par trois axes verticaux descendants t l'axe du temps pour illustrer les traitements effectués par le magnétoscope numérique DVCR 203, le dispositif de présentation 202 et la carte terminal/convertisseur 211 ainsi que les échanges entre ces éléments lorsqu'un nouveau contenu provenant du domaine N1 est diffusé sur le réseau domestique numérique du domaine N2.

Dans un premier temps, l'utilisateur insère par exemple la cassette vidéo contenant le programme vidéo enregistré dans le domaine N1, dans le magnétoscope numérique 203 du domaine N2. Le magnétoscope diffuse alors

classiquement sur le réseau du domaine N2 les données enregistrées sur la cassette.

Nous supposons que l'utilisateur souhaite visualiser le contenu sur le dispositif de présentation 202. Il réglera donc ce dispositif sur le canal de diffusion du magnétoscope numérique 203 pour recevoir les données.

Ces données diffusées à l'étape 401 de la figure 4 contiennent des paquets de données tels que le paquet suivant :

LECM1 | E{CW}(<données>), soit

E{K<sub>N1</sub>}(K<sub>C</sub>) | E{K<sub>C</sub>}(CW) | Champ d'intégrité | E{CW}(<données>), où  
le Champ d'intégrité est calculé comme suit :

Hash (E{K<sub>N1</sub>}(K<sub>C</sub>) | CW),

avec « Hash (x) » qui représente une fonction de hachage, c'est à dire une fonction mathématique qui transforme un ensemble de données d'entrée « x » en un ensemble de données « y » de taille fixe, souvent inférieure à la taille des données d'entrée, et représentatives des données d'entrées ; cette fonction est de plus une fonction à sens unique (« one way function » en anglais) c'est à dire que, connaissant « y », il est impossible de retrouver « x » tel que  $y = \text{Hash}(x)$ . Préférentiellement, nous utilisons la fonction SHA-1 décrite dans le document « *Secure Hash Standard, FIPS PUB 180-1, National Institute of Standard Technology, 1995* ».

Lorsqu'un tel paquet de données est reçu dans le dispositif de présentation 202, le module « Unité LECM » 223 extrait le message LECM1 du paquet de données et le transmet au module terminal 222.

Celui-ci va tout d'abord détecter à l'étape 402 que ce message LECM1 provient d'un domaine différent du domaine N2.

Pour cela, selon une première variante de réalisation préférée, le message LECM1 contient en outre dans sa partie en clair, c'est à dire dans sa partie qui n'est pas chiffrée par la clé K<sub>C</sub>, un identifiant de domaine ID<sub>N1</sub>. Cet identifiant identifie de manière unique le domaine N1 et est par exemple le résultat d'une fonction de hachage appliquée à la clé secrète du domaine N1, K<sub>N1</sub>. L'identifiant ID<sub>N1</sub> est contenu dans toute carte terminal d'un dispositif de présentation du domaine N1. Il est également contenu dans ce cas dans la carte terminal/convertisseur 211.

La carte terminal 221 du dispositif de présentation 202 contient aussi, en plus de la clé secrète du domaine N2, un identifiant du domaine N2 : ID<sub>N2</sub>. Le module terminal 222 compare donc l'identifiant ID<sub>N1</sub> contenu dans le message LECM1 avec l'identifiant contenu dans la carte terminal/convertisseur ID<sub>N2</sub>. Lorsque les deux identifiants sont différents, le module terminal 222 en

déduit que le message LECM1 reçu provient d'un domaine différent du domaine N2.

5 Selon une deuxième variante de réalisation, le message LECM1 ne contient pas d'identifiant de domaine. Le module terminal 222 utilisera dans ce cas le Champ d'intégrité du message LECM1 pour vérifier si ce message provient du domaine N2 ou non.

10 En effet, si le module terminal 222 déchiffre le message LECM1 avec la clé  $K_{N2}$  et applique la fonction de hachage « Hash(x) » précitée aux données déchiffrées, le résultat obtenu sera différent du Champ d'intégrité du message LECM1 et le module terminal en déduira que le message LECM1 provient d'un domaine différent de N2.

15 A l'étape suivante 403, le module terminal 222 génère un nombre aléatoire R. Ce nombre est préférentiellement généré par un générateur de nombres pseudo-aléatoires bien connu en soi. Le nombre R est un challenge utilisé pour prévenir les « replay attacks » (attaques consistant à rejouer des messages enregistrés). Le nombre R est mémorisé temporairement à l'étape 403 dans une zone de mémoire sécurisée de la carte 221.

20 Le dispositif de présentation 202 diffuse ensuite sur le réseau, à l'étape 404, un message contenant les données suivantes :

$R \mid E\{K_{N1}\}(K_C) \mid ID_{N1}$

L'identifiant  $ID_{N1}$  n'est inclus dans ce message que dans la première variante de réalisation décrite ci-dessus.

25 Cette diffusion est effectuée en utilisant le canal asynchrone du bus 204 par lequel transitent habituellement les messages de commande (l'envoi par le canal asynchrone du bus 204 est représenté par une flèche en pointillés à la figure 4).

Le dispositif source 201 qui reçoit ce message le transmet à la carte terminal/convertisseur 211.

30 L'étape suivante 405 n'a lieu que dans le cadre de la première variante de réalisation précitée et consiste à vérifier que l'identifiant inclus dans le message reçu à l'étape 404 est identique à celui contenu dans la carte terminal/convertisseur 211. Si les deux identifiants ne sont pas identiques, alors le procédé s'arrête car la carte terminal/convertisseur 211 n'est pas en mesure de déchiffrer l'information  $E\{K_{N1}\}(K_C)$ . Si les identifiants sont identiques, par 35 contre, le procédé se poursuit par l'étape 406 lors de laquelle la carte terminal/convertisseur déchiffre  $E\{K_{N1}\}(K_C)$  à l'aide de la clé  $K_{N1}$  pour obtenir la clé  $K_C$ .



Dans le cas où la seconde variante de réalisation est utilisée, l'étape 405 n'a pas lieu et toute carte terminal/convertisseur raccordée au réseau du domaine N2 effectuera l'étape 406 et les suivantes 407 et 408.

- 5 A l'étape 407, la carte terminal/convertisseur chiffre les données R et  $K_C$  avec la clé  $K'_C$  puis elle construit le message suivant :

$E\{K_{N2}\}(K'_C) \mid E\{K'_C\}(R \mid K_C)$

qu'elle transmet au dispositif de présentation 202, toujours via le canal asynchrone du bus 204, à l'étape 408.

- 10 A l'étape 409, le module terminal 222 déchiffre  $E\{K_{N2}\}(K'_C)$  avec la clé  $K_{N2}$  pour obtenir la clé  $K'_C$  avec laquelle il déchiffre  $E\{K'_C\}(R \mid K_C)$  pour obtenir  $R \mid K_C$  à l'étape suivante 410.

- 15 Ensuite, à l'étape 411, le module terminal 222 vérifie que le nombre R retrouvé à l'étape 410 est bien le même que celui qui a été généré et mémorisé à l'étape 403. Si ce n'est pas le cas, le procédé s'arrête car cela signifie que le message reçu à l'étape 408 n'est pas valide.

Si la vérification est positive, le procédé se poursuit à l'étape 412 par le déchiffrement du message LECM1 à l'aide de la clé  $K_C$  obtenue à l'étape 410. Plus précisément, l'information  $E\{K_C\}(CW)$  est déchiffrée pour obtenir le mot de contrôle en clair CW.

- 20 Le module terminal 222 vérifie également à l'étape 412 l'intégrité du message LECM1 en calculant :

$\text{Hash}(E\{K_{N1}\}(K_C) \mid CW)$  à partir des données déchiffrées ci-dessus et en comparant ce résultat au Champ d'intégrité du message LECM1.

- 25 Lorsque la deuxième variante de réalisation mentionnée ci-dessus est mise en œuvre, le dispositif de présentation 202 peut éventuellement recevoir plusieurs messages du type de celui envoyé à l'étape 408 si plusieurs cartes terminal/convertisseur sont raccordées au réseau du domaine N2. Dans ce cas, le module terminal 222 effectue les étapes 409 à 412 pour chaque message reçu à l'étape 408 et lorsque la vérification de l'intégrité du message LECM1 est correcte, le module terminal en déduit que le message reçu à l'étape 408 est celui issu de la carte terminal/convertisseur provenant du domaine N1.

- 35 Si la vérification d'intégrité échoue dans tous les cas, alors le procédé est arrêté. On peut prévoir dans ce cas d'afficher un message d'avertissement à destination de l'utilisateur.

Sinon, le module terminal 222 transmet le mot de contrôle CW déchiffré au module « Unité LECM » du récepteur de télévision 220 et celui-ci

peut ainsi désembrouiller, à l'étape 413, les données du paquet de données reçu à l'étape 401.

Le dispositif de présentation 202 est aussi capable, grâce à la clé  $K_C$  qu'il mémorise temporairement, de déchiffrer les paquets de données suivants du contenu diffusé par le magnétoscope numérique 203 tant que les messages LECM1 de ces paquets sont protégés par la même clé  $K_C$ . Si jamais la clé  $K_C$  change alors les étapes 403 à 412 sont répétées pour que le dispositif de présentation 202 reçoive la nouvelle clé  $K_C$  de la carte terminal/convertisseur 211.

Ensuite, lorsque l'ensemble des paquets de données formant le contenu ont été reçus et déchiffrés par le dispositif de présentation 202, ce dernier efface de sa mémoire à l'étape 414 le nombre  $R$  et la clé  $K_C$  qu'il avait mémorisés temporairement pour effectuer les calculs ci-dessus.

A la figure 2, nous avons illustré un mode de réalisation dans lequel la carte terminal/convertisseur 211 est insérée dans un dispositif source du domaine  $N_2$ , à la place de la carte convertisseur qui s'y trouve normalement.

Mais il est également possible, dans un second mode de réalisation, d'insérer la carte terminal/convertisseur dans un dispositif de présentation du domaine  $N_2$ , à la place de la carte terminal qui s'y trouve habituellement. Le procédé fonctionnera de la même manière que ce qui a été décrit en liaison avec les figures 3 et 4. Cependant, dans ce cas, il est nécessaire naturellement que le domaine  $N_2$  comprenne au moins deux dispositifs de présentation de manière à ce qu'au moins un des dispositifs puisse conserver sa carte terminal contenant la clé  $K_{N_2}$  du domaine pour mettre en œuvre les étapes qui sont illustrées aux figures 3 et 4.

L'invention ne se limite pas aux exemples de réalisation qui viennent d'être décrits. En particulier, elle s'applique également aux réseaux domestiques numériques dans lesquels les données (notamment les messages LECM) sont protégées à l'aide d'une paire de clés asymétriques spécifique au domaine auquel appartient le réseau, la clé publique du réseau étant contenue dans les dispositifs sources pour chiffrer les données et la clé privée étant contenue dans les dispositifs de présentation pour déchiffrer les données. Dans ce cas, la carte terminal/convertisseur doit contenir, après la phase d'initialisation, la clé privée du premier domaine  $N_1$  et la clé publique du second domaine  $N_2$  pour être en mesure de déchiffrer les données chiffrées pour le

premier domaine et de les re-chiffrer de manière à ce qu'elles soient déchiffrables par un dispositif de présentation du second domaine.

- De même, l'invention s'applique aussi dans un autre cas particulier
- 5 où des données numériques, protégées par un système d'accès conditionnel d'un fournisseur de contenu, sont reçues dans un domaine donné N2 et sont directement enregistrées dans un dispositif d'enregistrement du domaine N2 sans avoir été au préalable « converties » par un module convertisseur du domaine N2 pour être relues dans le domaine N2. Lorsque ces données
- 10 enregistrées sont ultérieurement reçues par un dispositif de présentation du domaine N2 pour être présentées à un utilisateur, ce dispositif de présentation n'est pas capable de déchiffrer les ECM contenant les mots de contrôle CW protégés par un secret propre au fournisseur de contenu (typiquement, la clé  $K_F$  apparaissant à la figure 1 dans le module CA 14). On considère dans ce cas
- 15 que le « premier domaine » au sens de la présente invention est celui du fournisseur de contenu. Le dispositif de présentation diffuse alors sur le réseau du domaine N2 les messages ECM pour que ceux-ci soient convertis par un module convertisseur du domaine N2 (associé à un module d'accès conditionnel du fournisseur de contenu) en messages LECM déchiffrables à
- 20 l'aide du secret du domaine N2.

## REVENDICATIONS

1. Procédé de traitement de données (LECM1), chiffrées selon un procédé de chiffrement propre à un premier domaine de sorte qu'elles ne puissent être déchiffrées qu'à l'aide d'un premier secret ( $K_{N1}$ ) propre audit premier domaine, lesdites données étant reçues dans un dispositif de présentation (202) raccordé à un réseau appartenant à un second domaine, caractérisé en ce qu'il comporte les étapes consistant pour le dispositif de présentation à :
- 5 (a) transmettre (404) à un dispositif de traitement (211) raccordé au réseau une partie ( $E\{K_{N1}\}(K_C)$ ) au moins desdites données chiffrées ;
- (b) recevoir (408) dudit dispositif de traitement (211) au moins un élément ( $E\{K_{N2}\}(K'_C)|E\{K'_C\}(K_C)$ ) permettant de déchiffrer lesdites données reçues à l'aide d'un second secret ( $K_{N2}$ ) propre audit second domaine, ledit
- 15 second secret étant contenu dans le dispositif de présentation.
2. Procédé selon la revendication 1, caractérisé en ce que les données reçues dans le dispositif de présentation (202) sont chiffrées à l'aide d'une première clé symétrique ( $K_C$ ), ladite première clé symétrique étant reçue
- 20 avec lesdites données sous forme chiffrée ( $E\{K_{N1}\}(K_C)$ ) à l'aide du premier secret ( $K_{N1}$ ) ;
- en ce que l'étape (a) consiste à transmettre au dispositif de traitement la première clé symétrique chiffrée ( $E\{K_{N1}\}(K_C)$ ) à l'aide du premier secret ; et
- 25 en ce que l'étape (b) consiste à recevoir du dispositif de traitement :
- ladite première clé symétrique chiffrée ( $E\{K'_C\}(K_C)$ ) à l'aide d'une seconde clé symétrique ( $K'_C$ ) ; et
  - la seconde clé symétrique chiffrée ( $E\{K_{N2}\}(K'_C)$ ) à l'aide du second secret ( $K_{N2}$ ) propre au second domaine.
- 30
3. Procédé selon la revendication 2, caractérisé en ce qu'il comporte en outre les étapes consistant pour le dispositif de présentation à :
- (c) déchiffrer (409), à l'aide du second secret ( $K_{N2}$ ), la seconde clé symétrique ( $K'_C$ ) chiffrée ;
- 35 (d) déchiffrer (410), à l'aide de la seconde clé symétrique ( $K'_C$ ), la première clé symétrique ( $K_C$ ) chiffrée ; et
- (e) déchiffrer les données reçues (LECM1) par ledit dispositif de présentation à l'aide de la première clé symétrique ( $K_C$ ).

4. Procédé selon la revendication 3, caractérisé en ce qu'il comporte en outre, avant l'étape (a), une étape (403) consistant pour le dispositif de présentation à générer un nombre aléatoire (R),

5           ledit nombre aléatoire (R) étant transmis au dispositif de traitement, à l'étape (a), avec le chiffrement ( $E\{K_{N1}\}(K_C)$ ) de la première clé symétrique ;

          et en ce que les données reçues à l'étape (b) contiennent un nombre aléatoire (R) et la première clé symétrique ( $K_C$ ) chiffrés ( $E\{K'_C\}(R|K_C)$ ) à l'aide de la seconde clé symétrique ( $K'_C$ ) ;

10           l'étape (d) comprenant également le déchiffrement, à l'aide de la seconde symétrique ( $K'_C$ ), du nombre aléatoire (R) chiffré reçus à l'étape (b) ; et

          le procédé comportant en outre, avant l'étape (e), une étape de vérification (411) que le nombre aléatoire (R) déchiffré à l'étape (d) est identique au nombre aléatoire (R) généré avant l'étape (a) ; l'étape (e) n'étant

15 effectuée qu'en cas de vérification positive.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'un identifiant de domaine ( $ID_{N1}$ ) est contenu dans les données (LECM1) reçues par le dispositif de présentation (202) et

20           en ce que ledit identifiant de domaine est transmis au dispositif de traitement (211) lors de l'étape (a) ;

          l'étape (b) n'étant effectuée que si ledit dispositif de traitement contient le même identifiant de domaine.

25

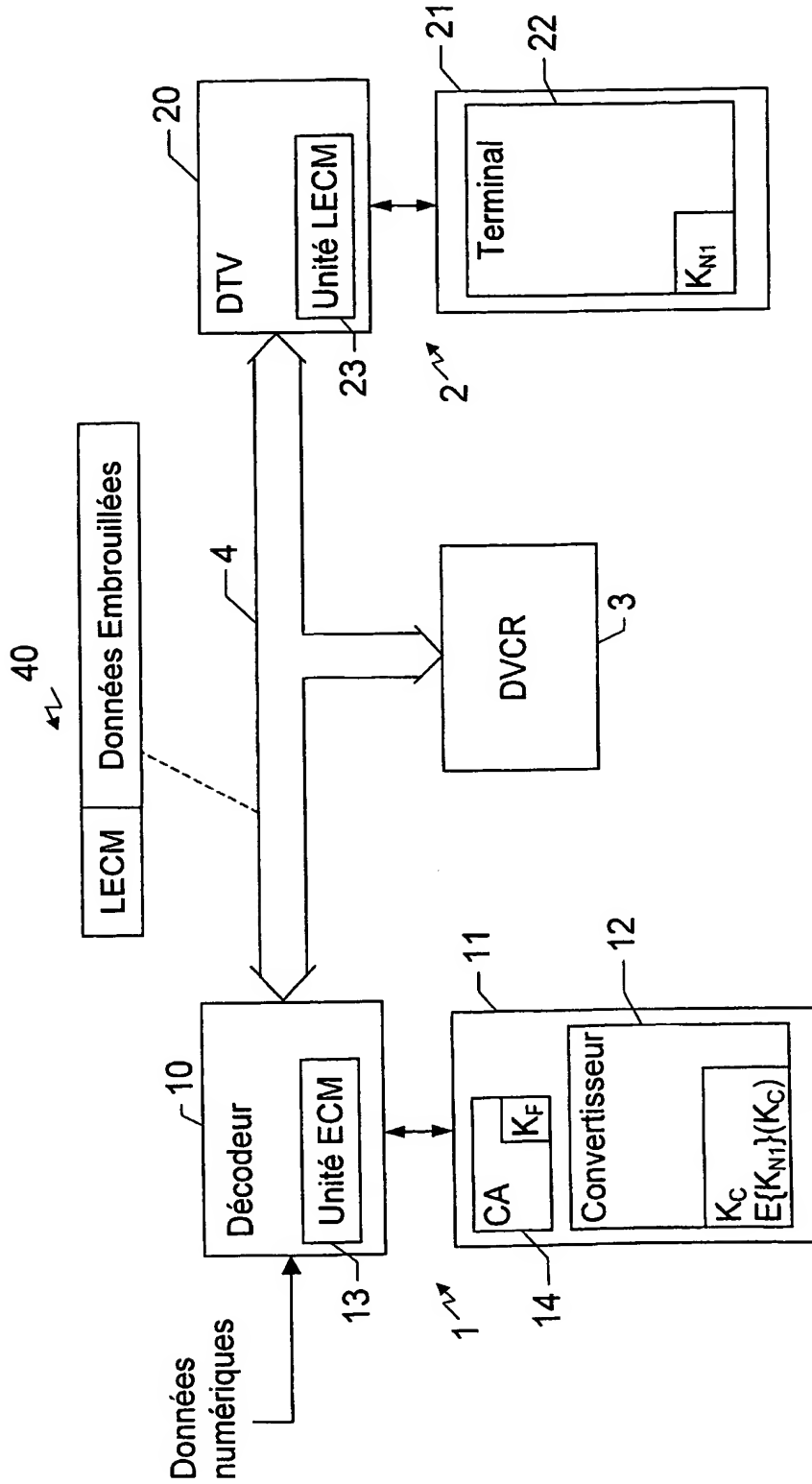


Fig. 1

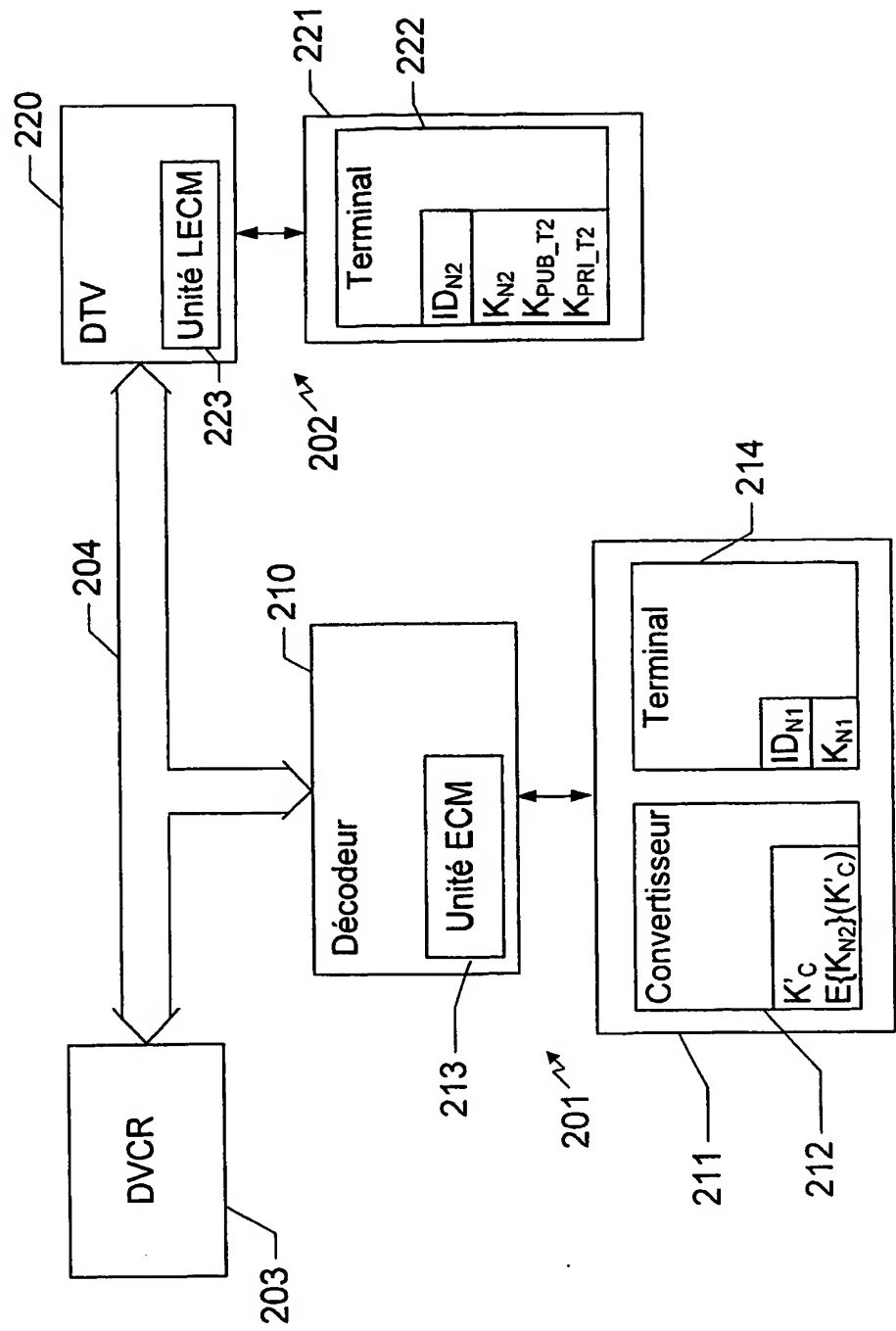


Fig. 2

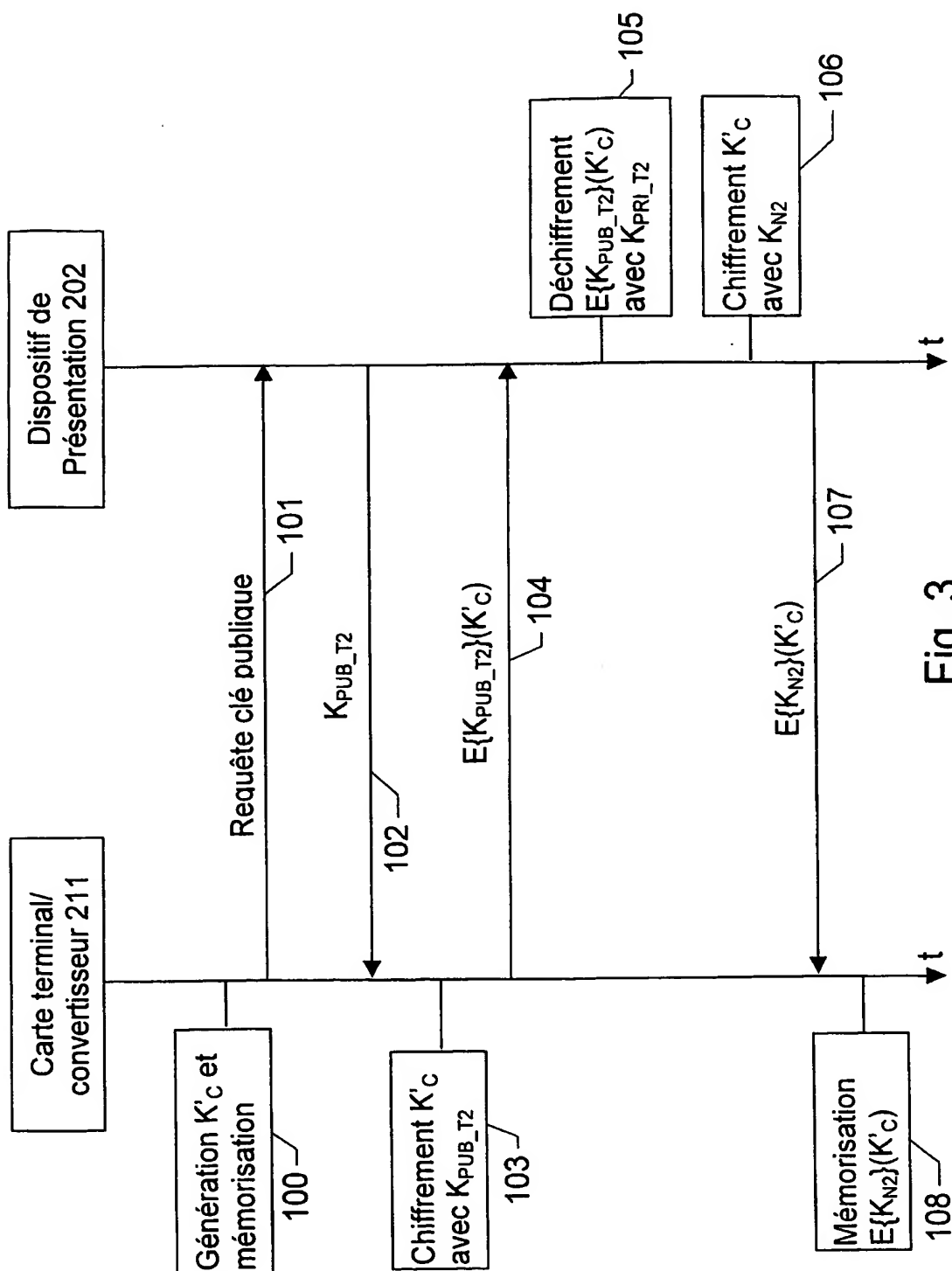


Fig. 3



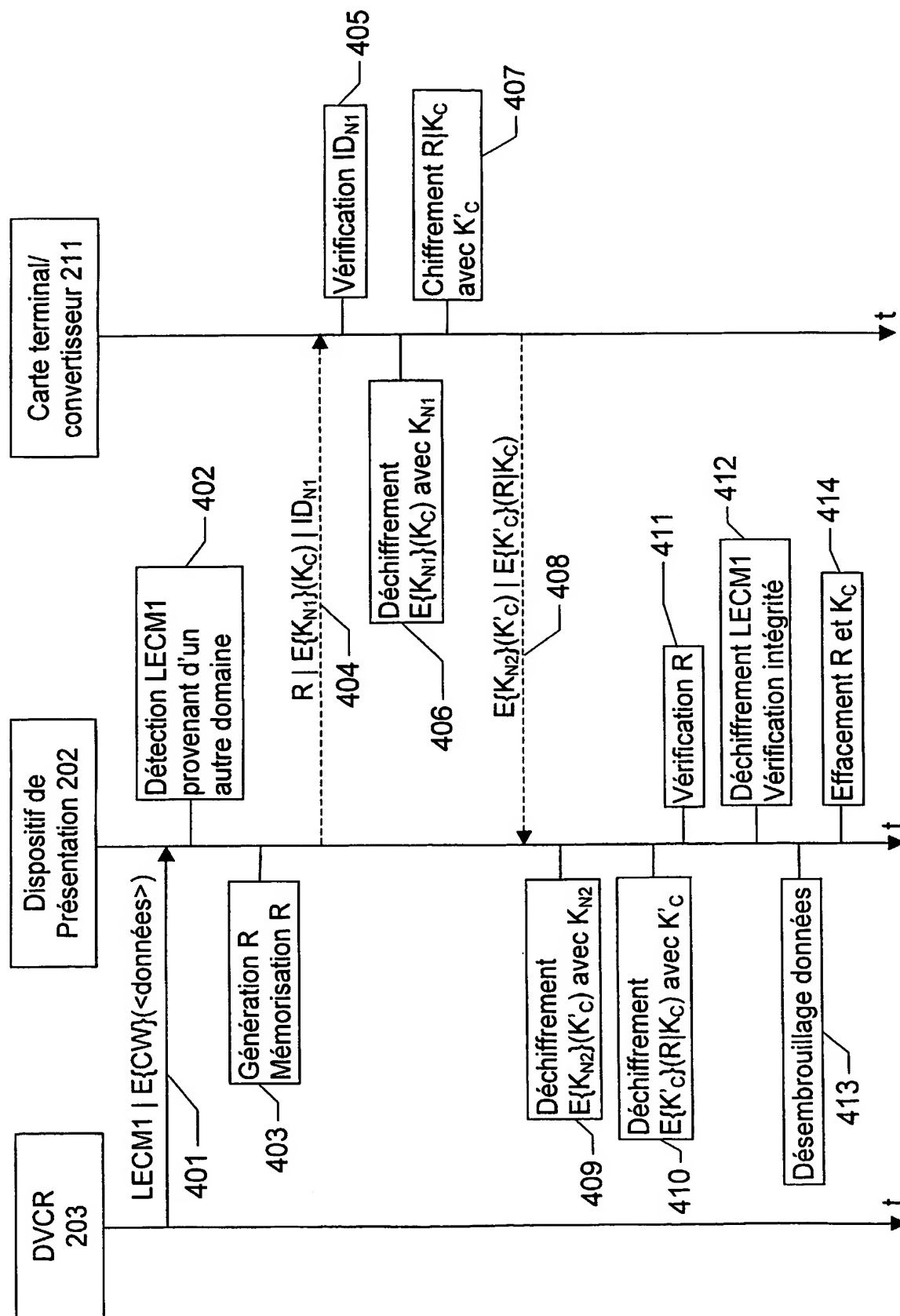


Fig. 4

PCT/FR 03/00583

## INTERNATIONAL SEARCH REPORT

Inter: 11 Application No

PCT/FR 03/00583

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 62505 A (THOMSON MULTIMEDIA SA ; FURON TEDDY (FR); QUES FLORENCE (FR); ANDRE) 19 October 2000 (2000-10-19) page 3, line 28 - line 36 figure 1 -----	1-5

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 93/00583

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0056068	A	21-09-2000	AU 759546 B2 17-04-2003
			AU 3629100 A 04-10-2000
			CA 2366301 A1 21-09-2000
			CN 1343420 T 03-04-2002
			EP 1169856 A1 09-01-2002
			JP 2002539724 T 19-11-2002
			NZ 513903 A 28-09-2001
			WO 0056068 A1 21-09-2000
EP 0858184	A	12-08-1998	IL 120174 A 28-10-1999
			EP 0858184 A2 12-08-1998
			US 6178242 B1 23-01-2001
			GB 2322030 A ,B 12-08-1998
WO 0062505	A	19-10-2000	FR 2792482 A1 20-10-2000
			AU 3658900 A 14-11-2000
			CN 1354946 T 19-06-2002
			WO 0062505 A1 19-10-2000
			EP 1169831 A1 09-01-2002
			JP 2002542672 T 10-12-2002

## RAPPORT DE RECHERCHE INTERNATIONALE

Den Internationale No

PCT/FR 03/00583

A. CLASSEMENT DE L'OBJET DE LA DEMANDE  
CIB 7 H04N7/16 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

## B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04N H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal

## C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 00 56068 A (THOMSON LICENSING SA ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET M) 21 septembre 2000 (2000-09-21) page 4, ligne 4 - ligne 14 page 5, ligne 1 - ligne 14 page 6, ligne 1 - ligne 12 page 7, ligne 8 - ligne 28 page 13, ligne 31 -page 14, ligne 27 figure 1B ---	1-5
A	EP 0 858 184 A (NDS LTD) 12 août 1998 (1998-08-12) colonne 1 -colonne 7, ligne 20 figures 1-5 ---	1-5
	-/--	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

## ° Catégories spéciales de documents cités:

- \*"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- \*"E" document antérieur, mais publié à la date de dépôt international ou après cette date
- \*"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- \*"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- \*"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- \*"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- \*"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- \*"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- \*"G" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

1 juillet 2003

Date d'expédition du présent rapport de recherche internationale

08/07/2003

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Tito Martins, J

# RAPPORT DE RECHERCHE INTERNATIONALE

Dem nternationale No

PCT/FR 03/00583

C.(suite) DOCUMENTS CONSIDERES COMM TINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>WO 00 62505 A (THOMSON MULTIMEDIA SA ; FURON TEDDY (FR); QUES FLORENCE (FR); ANDRE) 19 octobre 2000 (2000-10-19) page 3, ligne 28 - ligne 36 figure 1</p> <p>-----</p>	1-5

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. nternationale No

PCT/FR 03/00583

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0056068	A	21-09-2000	AU 759546 B2	17-04-2003
			AU 3629100 A	04-10-2000
			CA 2366301 A1	21-09-2000
			CN 1343420 T	03-04-2002
			EP 1169856 A1	09-01-2002
			JP 2002539724 T	19-11-2002
			NZ 513903 A	28-09-2001
			WO 0056068 A1	21-09-2000
EP 0858184	A	12-08-1998	IL 120174 A	28-10-1999
			EP 0858184 A2	12-08-1998
			US 6178242 B1	23-01-2001
			GB 2322030 A , B	12-08-1998
WO 0062505	A	19-10-2000	FR 2792482 A1	20-10-2000
			AU 3658900 A	14-11-2000
			CN 1354946 T	19-06-2002
			WO 0062505 A1	19-10-2000
			EP 1169831 A1	09-01-2002
			JP 2002542672 T	10-12-2002